



PRESENTATION NOTE OF THE LAW 43.20 ON TRUST SERVICES FOR ELECTRONIC TRANSACTIONS

The Law 43.20 on trust services for electronic transactions was unanimously adopted by the two chambers of Parliament respectively on December 8 and 15, 2020.

This law aims to establish a new legal framework to meet the needs of public and private economic actors, public administrations and citizens through the organization of electronic signatures, electronic seal, electronic time stamping, electronic registered delivery services and certificate services for website authentication.

It also aims to establish a less restrictive and more appropriate legal framework for the various transactions and to clarify the legal effect of the simple and advanced electronic signature, so that the legal effect of these two electronic signatures cannot be rejected or not accepted simply because they are presented in electronic form or because they do not meet the requirements for a qualified electronic signature.

It is also intended to extend the scope of the law to include documents issued by credit institutions and assimilated bodies

1. ELECTRONIC CERTIFICATION, A KEY ELEMENT OF DIGITAL TRUST

Morocco has made the strategic choice, for several years now, to rely on digital transformation as a real lever for economic and social growth. Among the objectives of its strategies are the accelerated development of the digital economy, human development through the reduction of the digital divide and finally the digital transformation of the Moroccan administration. This transformation is one of the pillars of the implementation of the law 55.19 on the reform of the administration and the simplification of procedures.

The economic and social development expected from digital transformation will only be possible if it benefits from a climate of trust for all digital services. Economic actors, administrations and public bodies need a reassuring legal environment to launch new services and, in the same way, citizens need to feel legally protected to carry out more and more operations online.

Digital trust is naturally reinforced by the appropriate use of electronic certification, a practice that was previously regulated by law 53.05 on the electronic exchange of legal data. However, given the evolution of needs, the necessity to define several levels of trust adapted to different uses, and the necessity to regulate new trust services such as electronic seal or electronic time stamps, the need to recast law 53.05 has been strongly felt.

2. A NEW LEGAL FRAMEWORK TO DEVELOP THE ELECTRONIC CERTIFICATION OFFER

2.1. The current regulation has been softened to allow general adoption of electronic certification

A first regulatory framework on the use of electronic certification was put in place, in our country, in 2007 with the law 53.05 on the electronic exchange of legal data. Although this first regulatory framework was established, the fact is that electronic certification has not been developed to the level of the expectations and needs of citizens, economic actors or administrations. Indeed, the regulations established to manage the uses of electronic certification, while seeking to provide the greatest possible security to users, were not flexible enough to encourage the widespread development of electronic certification.

Added to this rigidity is the absence of large-scale digitalization projects based on electronic certification. The current market remains modest to allow industrialization and enrichment of the current



offer. This offer is currently focused on secure signatures, which cannot be adopted for the majority of uses due to its complexity. As such, the majority of secure certificates put into circulation to date by the approved service provider have mainly been produced within the framework of a few public initiatives (Taxes, Customs, public procurement, etc.).

Based on these facts, it was established that the regulations and the digital trust ecosystem needed to evolve to better meet the expectations of public and private economic actors and citizens. With regard to the regulations, the alternatives to the secure signature were on one hand not sufficiently regulated to be perceived as legally valid and on the other hand, the only “secure” signature proved to be too restrictive to generalize the uses.

In addition, the Law 53.05 did not provide the desired clarity on the probative force of electronic certificates used for signing when they are not “secure” and did not deal with all of the trust services.

2.2. A new legal framework that meets the needs expressed by economic actors and administrations

Law 43.20 was drafted following the High Royal Assent, following a study carried out by the National Defense Administration to define a roadmap on the evolution of the digital certification offer in our country.

From the collection of needs to the development of this roadmap, many economic players were met in order to identify their specific needs and assess the maturity of digital uses and expectations in terms of digital trust. They were asked about their vision of the current development of electronic certification in Morocco and the possible obstacles encountered, as well as their future needs in terms of electronic certification.

At the end of these consultations, an inventory of current uses was drawn up, providing a concrete vision of the existing infrastructures as well as the desire of many players to dematerialize their services.

2.3. A legal framework enriched by various and pragmatic international approaches and initiatives

In parallel to the above-mentioned consultations, a review of certain international legal frameworks and initiatives from countries such as the United States, Canada, France, Malaysia, and South Korea was conducted in order to enrich the study with varied and pragmatic approaches and initiatives.

In light of international developments in the field of digital trust, our country had to upgrade its legal framework to be consistent and comparable with that of its economic partners. With the emergence of dematerialized services, international regulations had to evolve in order to provide a legal framework adapted to the uses and guarantee the protection of users.

The European Union's eIDAS (Electronic Identification and Trust Services) regulation, which became applicable on July 1, 2016, has created increased trust in electronic transactions by providing a common foundation for countries in the European space and a more comprehensive framework for secure electronic interactions between citizens, businesses and public authorities through a multitude of trust services

2.4. A new legal framework, less restrictive, completer and more adapted to the variety of uses

The new legal framework introduces a less restrictive regime than the older one in order to allow the digitization of the majority of uses, often with low or medium stakes (unqualified level), while maintaining a high level of security regime, more strict and benefiting from a greater legal effect, in order to cover certain uses with higher stakes (qualified level for a maximum security).



It is in fact a question of affirming a legal framework that makes it possible to integrate all of these developments, while consolidating the achievements and capitalizing on the investments already made.

In addition, the Covid-19 pandemic has highlighted the need to rapidly develop online public services so that citizens can use them to address public authorities remotely and to enable public and private economic actors and the administration to develop numerous teleservices and thus contribute to accelerating the Kingdom's digital transformation.

In this sense, Law 43.20 removed the various legal obstacles identified to the development of the digital trust market in Morocco. The amendments made by this new law have made it possible to further regulate the unqualified levels by adding an intermediate level called "advanced" following the example of European regulations.

This level now meets the legal requirements for each type of transaction and covers most needs to ensure widespread adoption. It also allows a better legal recognition than the "simple" level. As such, three levels of electronic signatures were retained by law 43.20:

"Simple" level

- No specified technical or functional requirements, for simplified use;
- No presumption of reliability: the burden of proof is on the defendant.

"Advanced" level

- Better legal recognition than the simple level: technical and organizational requirements of intermediate level (in particular the use of an electronic certificate), more flexible than the qualified signature;
- Useful for the development of medium-level uses;
- No presumption of reliability: the burden of proof is on the defendant.

"Qualified" level

- Mandatory use of cryptographic products and a qualified electronic certificate;
- Benefit from the presumption of reliability;
- Useful for the development of high-stake uses;
- Includes the concepts of the "secure" signature.

In addition, the Law 43.20 upgraded the current framework by setting up additional trust services to meet the many needs expressed by economic players, administrations and new digital uses. These new services are: the validation and preservation of electronic signatures, electronic seal, electronic time stamps, electronic registered delivery services and certificate services for website authentication.

These additional trust services are included in law 43.20, and will be detailed in the application texts with reference to international standards for their implementation.

To this end, the Law 43.20 establishes also rules applicable to trust services and the providers that provide them.

In order to increase user confidence in these services, all trust service providers will be subject to the requirements of the new law, including security and accountability for their activities and services. However, given the type of services provided by trust services providers, a distinction should be made in terms of these requirements between accredited and non-accredited trust services providers. For this purpose, two regimes for the supervision of these service providers have been adopted: a regime with increased confidence but subject to strict requirements linked to obtaining approval, and a less restrictive regime without approval.



Regarding the control of cryptology, Law 43.20 adopted a legislative framework that limits the control, over cryptology, to what is likely to harm the preservation of the interests of the defense and the security of the State.

The law also extends the application of its provisions to acts established by credit institutions and similar organizations as well as real rights.

Finally, the Law 43.20 includes transitional provisions that guarantee legal security for entities that are already using secure certificates that were issued, prior to the adoption of this law, in accordance with the legislative requirements in force regarding the electronic exchange of legal data (Law 53.05).